



THE DEPUTY SECRETARY OF DEFENSE
WASHINGTON, D.C. 20301-1000

6 AUG 1997



MEMORANDUM FOR UNDER SECRETARIES OF DEFENSE

DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

INFO COPY: SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF

SUBJECT: Management Reform Memorandum #16 -- Identifying Requirements for the
Design, Development and Implementation of a DoD Public Key Infrastructure

The Department of Defense is taking major steps in reforming its paper-based processes. It is our plan to move from traditional paper based processes into an environment where data is moved electronically between users. As part of this effort, we have developed a position paper for the Department on digital signatures and commercial practices that I want to share with you. Jointly developed by my office and the Assistant Secretary of Defense for Command, Control, Communications, Computers and Intelligence (ASD(C3I)), the Defense Information Systems Agency (DISA) and the National Security Agency (NSA), this document serves to identify the baseline for the Department's transition to a paperless environment. A copy of the approved position paper is attached for your information.

Also attached is a copy of a DoD news release, "Travel System Adopts Digital Signature," advising of our intention to use digital signatures in the Department's travel reengineering process. This effort will provide valuable feedback to us on PKI and digital signature technology for the DoD. As we continue to use and learn more about this technology, we will export this concept to other applications.

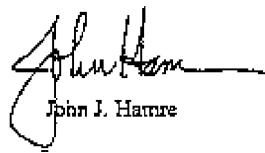
The ASD(C3I) has designated the DISA and NSA as the developers and implementers for the DoD Public Key Infrastructure (PKI). A DoD PKI will provide the data integrity, user identification and authentication, user on-repudiation, data confidentiality, encryption and digital signature services for our programs and applications, which use the DoD networks.

In order to identify the DoD PKI requirements, ensure interoperability with the PKI efforts of today, and to avoid stovepipe development activities, I have requested DISA to obtain input from each of you. The result of this survey, the long-term direction of the DoD PKI, and an

interim DoD PKI solution will be the topic of a PKI and Digital Signature Symposium jointly hosted by DISA and NSA during the next few months. This Symposium will be directed at the Principal Staff Assistants or designated Program Managers at the O6 level.

DISA's solicitation of your input will begin within the next couple of weeks. Please provide your full cooperation and prompt response. We value your input and expect the results to assist our efforts in protecting the Department's infrastructure, systems and data.

In approximately two weeks from the date of this memorandum, I will have my secretary arrange for a meeting with DISA to obtain a status report on how this effort is proceeding.



John J. Hamre

Position Paper

Department of Defense (DoD) Digital Signatures and Commercial Practices

Digital signature services are fundamental for secure electronic transactions, when there is a requirement to authenticate the parties conducting electronic transactions, and Guarantee the integrity of these transactions. A digital signature service requires, the choice of an algorithm (i.e., a Mathematical equation) for performing the digital signature process, and a supporting infrastructure to provide the electronic "Personality" (i.e., public key certificate) used to represent the individual in the signing and verification process. The signature algorithm relies on the infrastructure to provide the trusted association of the public key certificates to the individual users.

Within currently available technology, several algorithm options exist for implementing digital signature to include:

- Digital Signature Standard (DSS), as specified in FIPS 186, and
- Commercial signature algorithms, such as RSA Signature.

DSS is a Federal Information Processing Standard used within the federal government including DoD. Private sector organizations typically have adopted commercial signature algorithms such as RSA. To meet overall DoD objectives for secure electronic transactions, support for both DSS and commercial signature algorithms such as RSA is necessary. The Public Key Infrastructure (PKI) for the DoD, therefore must provide support for multiple levels of assurance and multiple signature approaches, to include both DSS and commercial signature algorithms.

DoD plans to use DSS for electronic transactions within the Department. Commercial signature algorithms (RSA, etc.) are appropriate for achieving interoperability with commercial trading partners. Business Area Managers should consider both DSS and commercial signature algorithms when modernizing.

A DoD-wide PKI will be established to support digital signature services as well as other security services such as encryption throughout the DoD. The National Security Agency (NSA) and Defense Information Systems Agency (DISA) jointly will undertake this responsibility. This PKI will satisfy the requirements of all DoD Business Areas, and provide for interoperability with non-DoD trading partners. To assure interoperability across the full spectrum of DoD requirements and functional areas, the DISA and NSA will establish a Technical Framework for the DoD PKI, defining a comprehensive set of infrastructure services along with implementation specifications. In establishing the Technical Framework for the DoD PKI, the DISA and NSA plan to fully integrate both the requirement for interoperability with federal and commercial PKIs, and the capability to outsource some or all DoD PKI services.

Although it embraces relatively "low-assurance" transactions, the Defense Travel System (DTS) requires integrity and/or authenticity services provided by digital signature. To be interoperable, both to DoD entities and with the private sector organizations, the DTS will support both DSS and RSA signatures. As the first step in establishing a DoD-wide PKI service, the DISA, with support from NSA, will enable a PKI for DTS efforts in Defense Travel Region Six as a starting point for using PKI services throughout the DoD. This initial service complements the "high-assurance" PKI services being established by the NSA and DISA to protect and provide access control for classified information.



IMMEDIATE RELEASE

July 2, 1997

No. 353-97
(703)695-0192(media)
(703)697-5737(public/industry)

TRAVEL SYSTEM ADOPTS DIGITAL SIGNATURES

The Department of Defense today announced a major step in reforming its travel procedures: the adoption of digital electronic signature for travel. Digital signatures will allow travelers to receive electronic authorization prior to a trip and permit them to sign their vouchers after the trip. These electronic "John Hancocks" create a secure and legal association between the traveler and the voucher information.

DoD will use the Federal Standard for Digital Signature (Federal Information Processing Standard 186) internally, but will also allow for interoperability with commercial algorithms such as RSA signature. Contractors will verify the accuracy and completeness of individual travel documents before payment.

"Adopting digital signature is a key move toward a paperless travel process in the Department of Defense," said Under Secretary of Defense (Comptroller) John Hamre and overseer of the Department's travel reengineering efforts. "We have to do business smarter and more efficiently--and these reforms in the Defense Travel System show we can."

The Defense Travel System is a large-scale attempt by the federal government to use digital signatures on travel claims. The new signature process is scheduled to be piloted first in the eleven state region of the DTS's Travel Region Six for trip planning and travel claims. Travel Region Six covers the states of Kentucky, Illinois, Indiana, Iowa, Michigan, Minnesota, Missouri, Nebraska, North Dakota, South Dakota and Wisconsin. The region includes more than 200,000 travelers and their authorizing officials. Phase in of the signature process starts in April 1998. Following successful implementation of the pilots within Region Six, the new procedures will be implemented rapidly throughout the Department.

Acceptance of digital signatures in the travel process could have much wider applications in reforming buying practices in the Department of Defense. The Defense Travel Service effort is serving as a practical approach for digital signature certificates, including commercial infrastructures and services, that could eventually be used in Department-wide electronic commerce efforts.

-END-

INTERNET AVAILABILITY: This document is available on DefenseLINK, a World Wide Web Server on the internet, at: <http://www.dtic.mil/defenselink/>